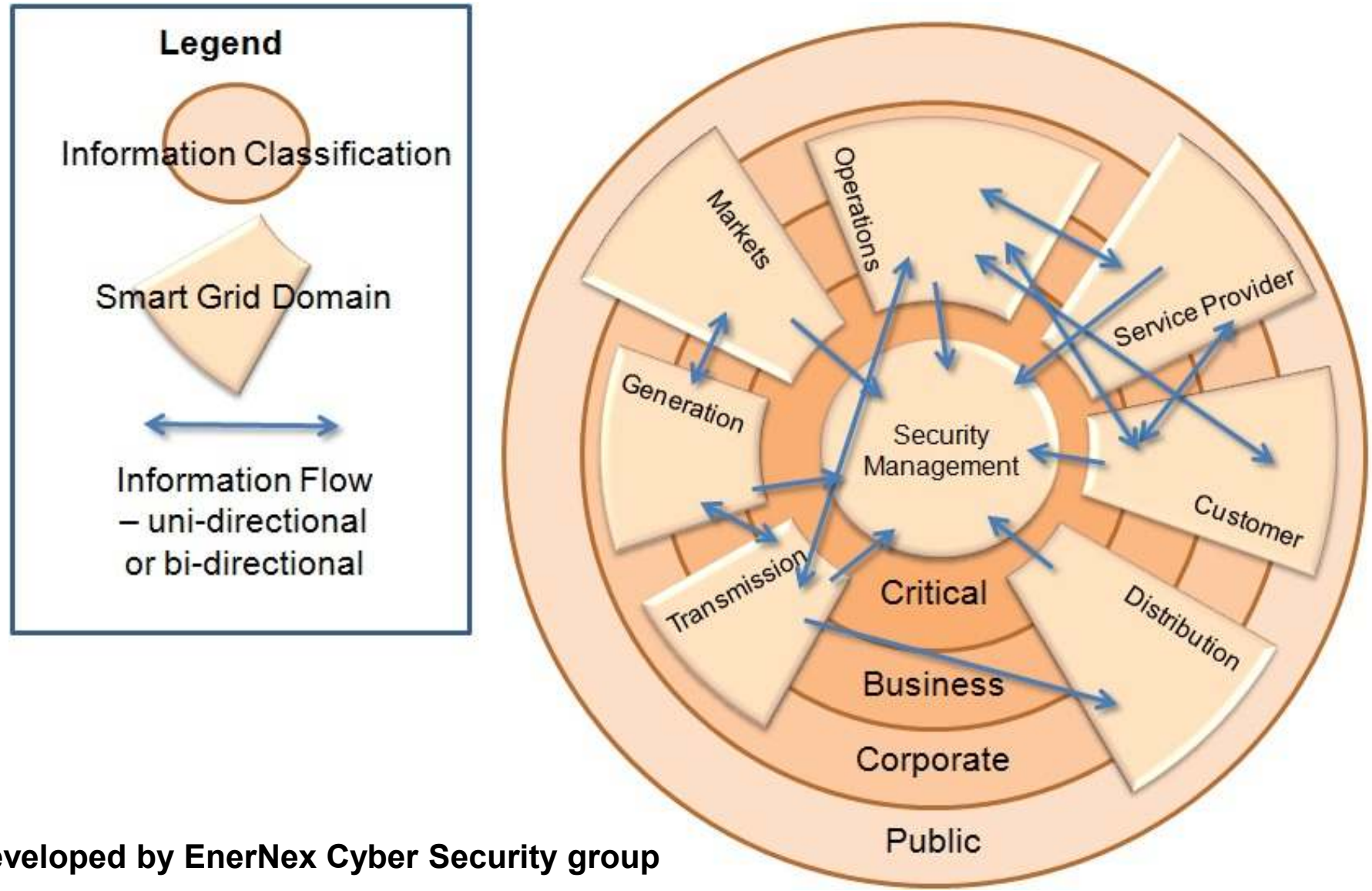
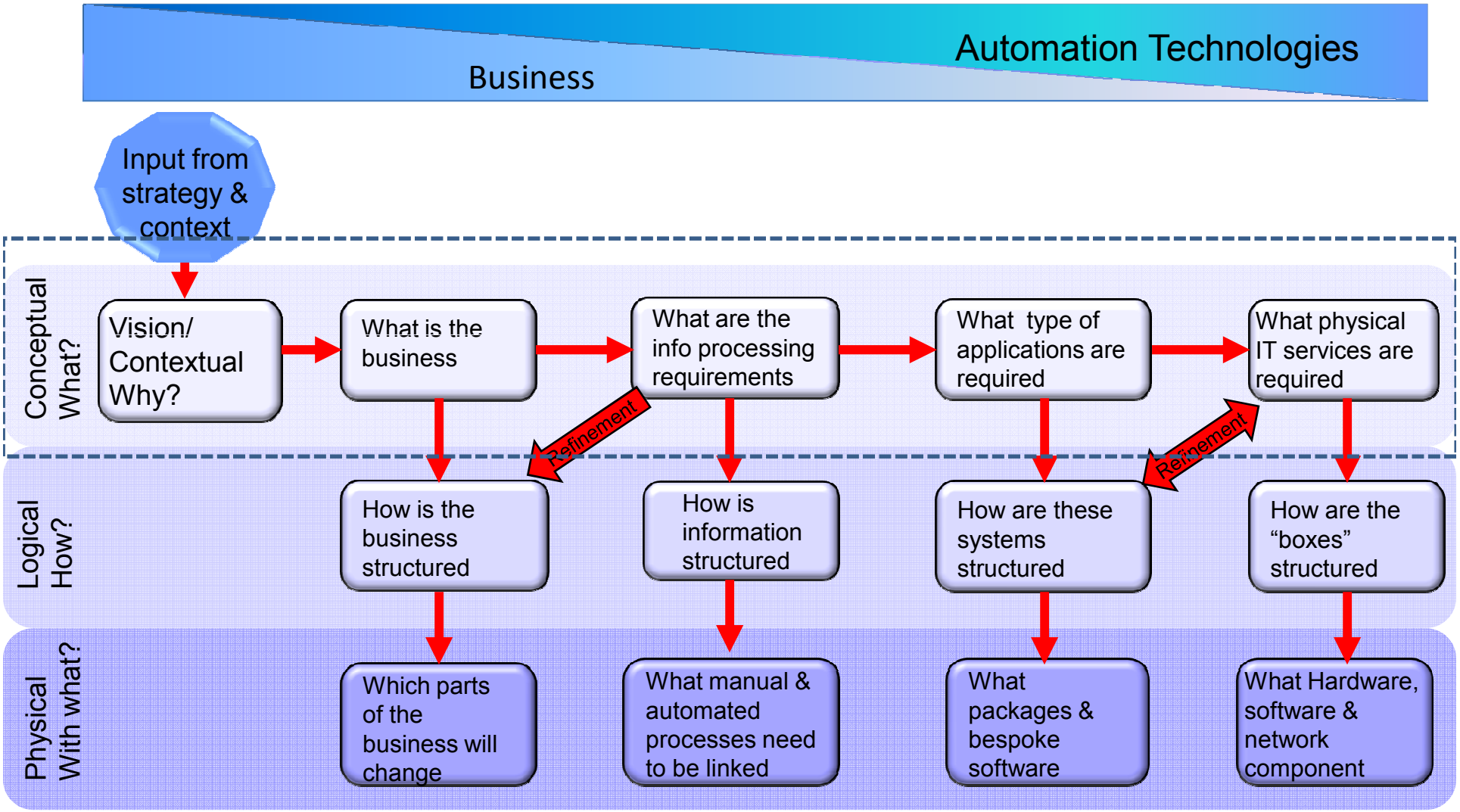
Drawings for the Security Architecture

Figure For showing that messages can cross domains and information classifications



Developed by EnerNex Cyber Security group

Architecture roadmap to show what conceptual architecture is



Developed by EnerNex Enterprise Architecture group

Based on NISTIR 7628 HLR – GRCs

NISTIR GRCs (1)

- SG.AC-1: Access Control Policy and Procedures
- SG.AC-2: Remote Access Policy and Procedures
- SG.AC-3: Account Management
- SG.AC-4: Access Enforcement
- SG.AC-18: Use of External Information Control Systems
- SG.AC-19: Control System Access Restrictions
- SG.AC-20: Publicly Accessible Content
- SG.AT-1: Awareness and Training Policy and Procedures
- SG.AT-2: Security Awareness
- SG.AT-3: Security Training
- SG.AT-4: Security Awareness and Training Records
- SG.AT-5: Contact with Security Groups and Associations
- SG.AT-6: Security Responsibility Training
- SG.AT-7: Planning Process Training
- SG.AU-1: Audit and Accountability
- SG.AU-5: Response to Audit Processing Failures
- SG.AU-6: Audit Monitoring, Analysis, and Reporting
- SG.AU-7: Audit Reduction and Report Generation
- SG.AU-8: Time Stamps
- SG.AU-9: Protection of Audit Information

NISTIR GRCs (2)

- SG.AU-10: Audit Record Retention
- SG.AU-11: Conduct and Frequency of Audits
- SG.AU-12: Auditor Qualification
- SG.AU-13: Audit Tools
- SG.AU-14: Security Policy Compliance
- SG.CA-1: Security Assessment and Authorization Policy and Procedures
- SG.CA-2: Security Assessments
- SG.CA-3: Continuous Improvement
- SG.CA-4: Information System Connections
- SG.CA-5: Security Authorization to Operate
- SG.CA-6: Continuous Monitoring
- SG.CM-1: Configuration Management Policy and Procedures
- SG.CM-2: Baseline Configuration
- SG.CM-3: Configuration Change Control
- SG.CM-4: Monitoring Configuration Changes
- SG.CM-5: Access Restrictions for Configuration Change
- SG.CM-6: Configuration Settings
- SG.CM-9: Addition, Removal, and Disposal of Equipment
- SG.CM-10: Factory Default Settings Management
- SG.CM-11: Configuration Management Plan

NISTIR GRCs (3)

- SG.CP-1: Continuity of Operations Policy and Procedures
- SG.CP-2: Continuity of Operations Plan
- SG.CP-3: Continuity of Operations Roles and Responsibilities
- SG.CP-4: Continuity of Operations Training
- SG.CP-5: Continuity of Operations Plan Testing
- SG.CP-6: Continuity of Operations Plan Update
- SG.CP-7: Alternate Storage Sites
- SG.CP-8: Alternate Telecommunication Services
- SG.CP-9: Alternate Control Center
- SG.CP-10: Smart Grid Information System Recovery and Reconstitution
- SG.CP-11: Fail-Safe Response
- SG.IA-1: Identification and Authentication Policy and Procedures
- SG.IA-2: Identifier Management
- SG.IA-3: Authenticator Management
- SG.ID-1: Information and Document Management Policy and Procedures
- SG.ID-2: Information and Document Retention
- SG.ID-3: Information Handling
- SG.ID-4: Information Exchange

NISTIR GRCs (4)

- SG.ID-5: Automated Labeling
- SG.IR-1: Incident Response Policy and Procedures
- SG.IR-2: Incident Response Roles and Responsibilities
- SG.IR-3: Incident Response Training
- SG.IR-4: Incident Response Testing and Exercises
- SG.IR-5: Incident Handling
- SG.IR-6: Incident Monitoring
- SG.IR-7: Incident Reporting
- SG.IR-8: Incident Response Investigation and Analysis
- SG.IR-9: Corrective Action
- SG.IR-10: Smart Grid Information System Backup
- SG.IR-11: Coordination of Emergency Response
- SG.MA-1: Smart Grid Information System Maintenance Policy and Procedures
- SG.MA-2: Legacy Smart Grid Information System Updates
- SG.MA-3: Smart Grid Information System Maintenance
- SG.MA-4: Maintenance Tools
- SG.MA-5: Maintenance Personnel
- SG.MA-6: Remote Maintenance
- SG.MA-7: Timely Maintenance
- SG.MP-1: Media Protection Policy and Procedures
- SG.MP-2: Media Sensitivity Level

NISTIR GRCs (5)

- SG.MP-3: Media Marking
- SG.MP-4: Media Storage
- SG.MP-5: Media Transport
- SG.MP-6: Media Sanitization and Disposal
- SG.PE-1: Physical and Environmental Security Policy and Procedures
- SG.PE-2: Physical Access Authorizations
- SG.PE-3: Physical Access
- SG.PE-4: Monitoring Physical Access
- SG.PE-5: Visitor Control
- SG.PE-6: Visitor Records
- SG.PE-7: Physical Access Log Retention
- SG.PE-8: Emergency Shutoff Protection
- SG.PE-9: Emergency Power
- SG.PE-10: Delivery and Removal
- SG.PE-11: Alternate Work Site
- SG.PE-12: Location of Smart Grid Information System Assets
- SG.PL-1: Strategic Planning Policy and Procedures
- SG.PL-2: Smart Grid Information System Security Plan
- SG.PL-3: Rules of Behavior
- SG.PL-4: Privacy Impact Assessment
- SG.PL-5: Security-Related Activity Planning
- SG.PM-1: Security Policy and Procedures

NISTIR GRCs (6)

- SG.PM-2: Security Program Plan
- SG.PM-3: Senior Management Authority
- SG.PM-4: Security Architecture
- SG.PM-5: Risk Management Strategy
- SG.PM-6: Security Authorization to Operate Process
- SG.PM-7: Mission/Business Process Definition
- SG.PM-8: Management Accountability
- SG.PS-1: Personnel Security Policy and Procedures
- SG.PS-2: Position Categorization
- SG.PS-3: Personnel Screening
- SG.PS-4: Personnel Termination
- SG.PS-5: Personnel Transfer
- SG.PS-6: Access Agreements
- SG.PS-7: Contractor and Third-Party Personnel Security
- SG.PS-8 : Personnel Accountability
- SG.PS-9: Personnel Roles
- SG.RA-1: Risk Assessment Policy and Procedures
- SG.RA-2: Risk Management Plan
- SG.RA-3: Security Impact Level
- SG.RA-4 : Risk Assessment
- SG.RA-5: Risk Assessment Update
- SG.RA-6: Vulnerability Assessment and Awareness

NISTIR GRCs (7)

- SG.SA-1: Smart Grid Information System and Services Acquisition Policy and Procedures
- SG.SA-2: Security Policies for Contractors and Third Parties
- SG.SA-3: Life-Cycle Support
- SG.SA-4: Acquisitions
- SG.SA-5: Smart Grid Information System Documentation
- SG.SA-6: Software License Usage Restrictions
- SG.SA-7: User-Installed Software
- SG.SA-8: Security Engineering Principles
- SG.SA-9: Developer Configuration Management
- SG.SC-1: System and Communication Protection Policy and Procedures
- SG.SC-13: Collaborative Computing
- SG.SI-1: System and Information Integrity Policy and Procedures
- SG.SI-2: Flaw Remediation
- SG.SI-3: Malicious Code and Spam Protection
- SG.SI-4: Smart Grid Information System Monitoring Tools and Techniques
- SG.SI-5: Security Alerts and Advisories
- SG.SI-6: Security Functionality Verification

Based on NISTIR 7628 HLR – GRCs

Need to be applied to whole conceptual security architecture

01/05/2012: Consensus for applying all GRCs to the whole conceptual security architecture

Based on NISTIR 7628 HLR – Technical Requirements

NISTIR Technical Requirements (1)

- SG.AC-5: Information Flow Enforcement
- SG.AC-6: Separation of Duties
- SG.AC-7: Least Privilege
- SG.AC-8: Unsuccessful Login Attempts
- SG.AC-9: Smart Grid Information System Use Notification
- SG.AC-10: Previous Logon Notification
- SG.AC-11: Concurrent Session Control
- SG.AC-12: Session Lock
- SG.AC-13: Remote Session Termination
- SG.AC-14: Permitted Actions without Identification or Authentication
- SG.AC-15: Remote Access
- SG.AC-16: Wireless Access Restrictions
- SG.AC-17: Access Control for Portable and Mobile Devices
- SG.AC-21: Passwords
- SG.AU-2: Auditable Events
- SG.AU-3: Content of Audit Records
- SG.AU-4: Audit Storage Capacity
- SG.AU-15: Audit Generation
- SG.AU-16: Non-Repudiation
- SG.IA-4: User Identification and Authentication

NISTIR Technical Requirements (1)

- SG.IA-5: Device Identification and Authentication
- SG.IA-6: Authenticator Feedback
- SG.SA-10: Developer Security Testing
- SG.SA-11: Supply Chain Protection
- SG.SC-2: Communications Partitioning
- SG.SC-3: Security Function Isolation
- SG.SC-4: Information Remnants
- SG.SC-5: Denial-of-Service Protection
- SG.SC-6: Resource Priority
- SG.SC-7: Boundary Protection
- SG.SC-8: Communication Integrity
- SG.SC-9: Communication Confidentiality
- SG.SC-10: Trusted Path
- SG.SC-11: Cryptographic Key Establishment and Management
- SG.SC-12: Use of Validated Cryptography
- SG.SC-14: Transmission of Security Parameters
- SG.SC-15: Public Key Infrastructure Certificates
- SG.SC-16: Mobile Code
- SG.SC-17: Voice-Over Internet Protocol
- SG.SC-18: System Connections
- SG.SC-19: Security Roles

NISTIR Technical Requirements (3)

- SG.SC-20: Message Authenticity
- SG.SC-21: Secure Name/Address Resolution Service
- SG.SC-22: Fail in Known State
- SG.SC-23: Thin Nodes
- SG.SC-24: Honeypots
- SG.SC-25: Operating System-Independent Applications
- SG.SC-26: Confidentiality of Information at Rest
- SG.SC-27: Heterogeneity
- SG.SC-28: Virtualization Technique
- SG.SC-29: Application Partitioning
- SG.SC-30: Information System Partitioning
- SG.SI-7: Software and Information Integrity
- SG.SI-8: Information Input Validation
- SG.SI-9: Error Handling

Based on NISTIR 7628 HLR – Technical Requirements

We will be applying, like the LICs, the Technical Requirements to the Security Services.

01/05/2012: Consensus for applying Technical Security Requirements to the security services and messages.

C-I-A Levels Applied to Message Types

- The next few slides will show what was the consensus on assigning a high, moderate, or low ranking to the confidentiality, availability, and integrity on each of our message types.

- Please note: We still have to harmonize and better genericize our message definitions.

Message C-I-A (1)

Message Name	Message Description	C	I	A
Acknowledgement	Recognition of receiving a message.	L	M	L
Alarm	An event based message via a system service to which a response is required.	M	M	H
Alert	An escalated or error event based message via a system service to which a response is NOT required. (INFORMATIONAL)	M	M	M
Audit	An event based message containing evidence directly pertaining to and resulting from the execution of a business process or system function.	M	H	L
Command	A sent statement or instruction that requires an action. (e.g. a command to change an encryption key, routing updates or to update software / firmware)	L	H	H
Contract	Enforceable agreement	H	H	L
Error	Response sent back from a command, statement, or instruction that did not execute properly. (e.g. communication error, message error, command not executed correctly)	L	H	M
Forecast	Forward looking time based estimates	M	M	M
Identification	Request to associate (e.g. join a program); Disassociate (e.g. remove from a program, remove from service, remove credentials); Identity (e.g. role), privileges, or rights information (credentials) E.G. SYSTEM TO SYSTEM	M	H	M

Message C-I-A (2)

Message Name	Message Description	C	I	A
Notification	Informational message about a situation (e.g. planned outage or device available)	L	M	L
Plan	List of steps and associated information for achieving an objective (e.g. switching plan, contingency plan, etc)	M	H	M
Policies	Rules that govern	M	H	L
Product	Item that can be bought or sold or Amount of money given or set as consideration for the sale of a specified thing (valuation)	L	M	M
Qualification	Verification of readiness. Can be positive or negative and includes metadata	L	M	M
Query	A request requiring a response of ~~configuration~~ information	L	M	L
Resources	Work units, logistics, and capabilities (similar to anything a field crew might use)	M	H	L
Response	Response sent back from the command, statement, or instruction requiring action; this could include identification and authentication responses	M	M	M
Schedule	Time based plan for a resource or entity	L	M	M

Message C-I-A (3)

Message Name	Message Description	C	I	A
Setting	Configuration; hardware or software attribute; ranges or limits within which things are allowed to vary; Connectivity and attributes of system, topology. Can include State and Configuration information; Attributes describing the surroundings of an entity (environment); Capabilities of device; Sensor values which can include supporting metadata including meta information to describe location (measurement)	L	H	H
Status	Current condition of an entity (e.g. on, off, broken…) can include meta information to describe location, but not additional configuration information	L	M	L
Time	Measure of chronology	L	H	H
Usage Information	Information can include meta information to describe location, but not additional configuration information (UTILITY)	M	H	M
Work Order	Request to have work performed. Can include asset/entity information (e.g. go here, do this)	L	M	M

C-I-A Levels Applied to Security Services

- The next few slides will show what was the consensus on assigning a high, moderate, or low ranking to the confidentiality, availability, and integrity on each of our security services.

- Please note: We still have to harmonize and better genericize our security service definitions.

Security Service C-I-A (1)

Security Service	C	I	A	Security Service Description
Access Control (logical and physical)	L	H	L	Ensuring that resources are accessed only by an authorized identity.
Audit Trails	L	H	M	A record showing a what function or access was performed to smart grid resource at a given period of time
Authentication - Enterprise	M	H	M	Verifying the identity as a prerequisite for granting access to smart grid resources in the enterprise.
Authentication - Message Origin	M	H	M	Verifying the identity of a message originator as a prerequisite for granting access to a Smart Grid resource.
Authentication - Session	M	H	M	Verifying the identity as a prerequisite for granting access to resources in a Smart Grid information system session.
Authorization	M	H	M	Determining the identity attempting to access a smart grid resource and ensure that the identity has the right to execute the functions requested.
Availability / Reliability	L	M	H	Managing the operational capability of smart grid assets to ensure they are operational when accessed.
Certification - Enterprise Credentials	L	H	M	The assessments conducted in support of accreditations for enterprise credentials, conducting an impartial assessment of an enterprise credential
Certification - Enterprise Public Key	L	H	M	The assessments conducted in support of accreditations for enterprise public key credentials, conducting an impartial assessment of an enterprise public key credential.

Security Service C-I-A (2)

Security Service	C	I	A	Security Service Description
Certification and Accreditation	L	H	M	Evaluating, describing, testing and authorizing smart grid systems and services prior to or after a system is in operation.
Confidentiality - Message Contents	H	H	M	Ensuring the message contents is protected from unauthorized disclosure.
Confidentiality - Stored Data	H	H	M	Ensuring stored data is protected from unauthorized disclosure.
Confidentiality - Traffic Flow	H	H	M	Ensuring the information flow is hidden from unauthorized access.
Contingency Planning	L	H	H	Ensuring an alternate course of action is followed if operational failure or an existing situation changes.
Crisis Management	L	M	M	Managing the processes needed to handle serious incidents and is an escalation of incident response services.
Directory Service	M	H	H	Managing the data and basic units of information that are maintained within the directory.
Disaster Recovery	L	H	H	Ensuring the activation and implementation of measures to restart operational activities after an incident.
Enterprise Registration	M	H	M	Ensuring that each unique user, service, and device is authorized and documented at the enterprise level.
Enterprise Unique Naming	M	H	H	Ensuring that each user, service, and device have unique naming to prevent confusion over what is being referenced within the enterprise.

Security Service C-I-A (3)

Security Service	C	I	A	Security Service Description
Environment Security	M	H	H	Ensuring environmental services are operational.
Incident Response	H	H	H	Ensuring actions are activated in response to detected security events.
Incident Reporting	H	H	H	Ensuring reporting is activated in response to detected security events.
Integrity Protection - Hardware	M	H	M	Ensuring the hardware is not altered during implementation or operation.
Integrity Protection - Message	M	H	M	Ensuring the message and message contents were not altered during creation, transport, and storage.
Integrity Protection - Software	M	H	M	Ensuring the operational software / firmware is protected from malicious attacks and unauthorized alteration.
Integrity Protection - Stored Data	M	H	M	Ensuring stored data is protected from unauthorized alteration or deletion.
Intrusion Detection	M	H	M	Managing the collection, analysis, and reporting of detected anomalous events and feed into the incident response process.
Message Replay Protection	M	H	H	Ensuring a message in transit cannot be captured and retransmitted.
Non-Repudiation	H	H	H	Ensuring assurance that a user, service, or device cannot later deny a message was sent or received.
Personnel Security	H	H	M	Ensuring qualified personnel are retained to perform assigned responsibilities.

Security Service C-I-A (4)

Security Service	C	I	A	Security Service Description
Physical Security	L	H	H	Managing the security of smart grid assets to prevent physical damage.
Replication and Backup - Data	M	H	H	Ensuring smart grid data is recoverable following an incident.
Replication and Backup - Software	M	H	H	Ensuring smart grid software is recoverable following an incident.
Risk Management	M	M	H	Ensuring the identification, assessment, and prioritization of risks followed by the application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.
Security Alarm Management	M	H	H	Managing security alarms reported from users, services, and devices and feed into the incident response services.
Security Measurement and Metrics	M	H	M	Managing the smart grid security activities of the enterprise are collected and analyzed for reporting.
Security Monitoring	M	H	M	Ensuring the operations of security management services are built and implemented into the logical smart grid architecture.
Security Operations Management	M	H	M	Managing the operations of procedures and technical requirements for security services.
Security Policy Management	M	H	L	Managing the procedural and technical creation and implementation of security policies to users, services, and devices.
Security Provisioning	M	H	H	Ensuring the implementation of user, service or device configurations to match security requirements and roles.

Security Service C-I-A (5)

Security Service	C	I	A	Security Service Description
Security Service Management	M	H	H	Managing the configuration of a user, service or device to match security requirements and roles.
Security Training and Awareness	L	L	L	Managing the security and safety training and awareness for smart grid assets.
Software Licensing Protection	L	M	L	Managing the governance for the usage or redistribution of software.
System Audit	H	H	M	Managing the audit of the system controls throughout a smart grid device to evaluate their effectiveness and to recommend improvements.
System Configuration Protection	H	H	M	Managing the way smart grid devices are setup including but not limited to firmware, security and other possible settings.
Trusted Time	H	H	H	Ensuring the time source and service are protected from alteration.
User Interface for Security	L	M	M	Ensuring the user interface is easy to use and present no significant obstacles to smart grid activities.
User Support	L	M	M	Managing the operational user issues within smart grid devices and services related to security.

- Security services to be applied at
  - Enterprise level
  - Component level
  - Application level
  - All messages
- Consensus work for applying security services started 01/12/2012 and continued through 02/02/2012.

Yes or No Means

- A response of “Yes” means it is required to be defined for everything in the category, regardless of the business criticality and the C-I-A rankings.

- A response of “No” means it is optional to be defined for everything in the category. Depending upon the individual enterprise, smart grid component, smart grid application, or individual messages risk assessment, the business criticality or the C-I-A ranking it might be changed to a “Yes”.

Access Control (logical and physical)

- Ensuring that resources are accessed only by an authorized identity.

- Apply at Enterprise? ***Yes*** or No (public pay)
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Audit Trails

- A record showing a what function or access was performed to smart grid resource at a given period of time.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Authentication - Enterprise

- Verifying the identity as a prerequisite for granting access to smart grid resources in the enterprise.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? Yes or ***No (semi-single or single sign-on, could make this a yes)***
- Apply at SG Application? Yes or ***No (semi-single or single sign-on, could make this a yes)***
- Apply to ALL message types? Yes or ***No (semi-single or single sign-on, could make this a yes)***

Authentication - Message Origin

- Verifying the identity of a message originator as a prerequisite for granting access to a Smart Grid resource.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Authentication - Session

- Verifying the identity as a prerequisite for granting access to resources in a Smart Grid information system session.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Authorization

- Determining the identity attempting to access a smart grid resource and ensure that the identity has the right to execute the functions requested.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Availability / Reliability

- Managing the operational capability of smart grid assets to ensure they are operational when accessed.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Certification - Enterprise Credentials

- The assessments conducted in support of accreditations for enterprise credentials, conducting an impartial assessment of an enterprise credential.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Certification - Enterprise Public Key

- The assessments conducted in support of accreditations for enterprise public key credentials, conducting an impartial assessment of an enterprise public key credential.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Certification and Accreditation

- Evaluating, describing, testing and authorizing smart grid systems and services prior to or after a system is in operation.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Confidentiality - Message Contents

- Ensuring the message contents is protected from unauthorized disclosure.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Confidentiality – Stored Data

- Ensuring stored data is protected from unauthorized disclosure.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Confidentiality – Traffic Flow

- Ensuring the information flow is hidden from unauthorized access.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Contingency Planning

- Ensuring an alternate course of action is followed if operational failure or an existing situation changes.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Crisis Management

- Managing the processes needed to handle serious incidents and is an escalation of an event.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Directory Service

- Managing the data and basic units of information that are maintained within the directory.

- Should we delete this service, because it is really technology specific?
  - NO, because this works across many environments.

Directory Service

- Managing the data and basic units of information that are maintained within the directory.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Disaster Recovery

- Ensuring the activation and implementation of measures to restart operational activities after an event.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Should these services be merged?

- Enterprise Registration – Ensuring that an identity has unique naming to prevent confusion over what is being referenced within the enterprise.
- Enterprise Unique Naming – Ensuring that an identity has unique naming to prevent confusion over what is being referenced within the enterprise.
- NO, Registration is a superset of the unique naming

Enterprise Registration

- Ensuring that the unique identity is authorized and documented at the enterprise level.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Enterprise Unique Naming

- Ensuring that an identity has unique naming to prevent confusion over what is being referenced within the enterprise.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Environmental Security

- Ensuring environmental services are operational.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Incident Response

- Ensuring actions are activated in response to detected events.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Incident Reporting

- Ensuring reporting is activated in response to detected events.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Integrity Protection - Hardware

- Ensuring the hardware is not altered during implementation or operation.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Integrity Protection - Message

- Ensuring the message and message contents were not altered during creation, transport, and storage.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Integrity Protection - Software

- Ensuring the operational software / firmware is protected from malicious attacks and unauthorized alteration.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? Yes or ***No***
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Integrity Protection – Stored Data

- Ensuring stored data is protected from unauthorized alteration or deletion.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Intrusion Detection

- Managing the collection, analysis, and reporting of detected anomalous events and feed into the incident response and crisis management processes.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Message Replay Protection

- Ensuring a message in transit cannot be captured and retransmitted.

- Apply at Enterprise? Yes or ***No***
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Non-Repudiation

- Ensuring assurance that an identity cannot later deny an action was performed.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Personnel Security

- Ensuring qualified personnel are retained to perform assigned responsibilities.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Physical Security

- Managing the security of smart grid assets to prevent physical damage.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? Yes or ***No***
- Apply to ALL message types? Yes or ***No***

Replication and Backup - Data

- Ensuring smart grid data is recoverable following an event.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Replication and Backup - Software

- Ensuring smart grid software is recoverable following an event.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Risk Management

- Ensuring the identification, assessment, and prioritization of risks followed by the application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Security Alarm Management

- Managing security alarms reported from users, services, and devices and feed into the incident response and crisis management services.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Security Measurement and Metrics

- Managing the smart grid security activities of the enterprise are collected and analyzed for reporting.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Security Monitoring

- Ensuring the operations of security management services are built and implemented into the logical smart grid architecture.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? *Yes* or **No**

Security Operations Management

- Managing the operations of procedures and technical requirements for security services.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? *Yes* or **No**

Security Policy Management

- Managing the procedural and technical creation and implementation of enterprise security policies.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Security Provisioning

- Ensuring the implementation of user, service or device configurations to match security requirements and roles.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Security Service Management

- Managing the configuration of a user, service or device to match security requirements and roles.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Security Training and Awareness

- Managing the security and safety training and awareness for smart grid assets.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Software Licensing

- Managing the governance for the usage or redistribution of software.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

System Audit

- Managing the audit of the system controls throughout a smart grid device to evaluate their effectiveness and to recommend improvements.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

System Configuration Protection

- Managing the way smart grid devices are setup including but not limited to firmware, security and other possible settings.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? Yes or ***No***

Time Synchronization

- Ensuring the time source and service are protected from alteration.

- Apply at Enterprise? ***Yes*** or No
- Apply at SG Component? ***Yes*** or No
- Apply at SG Application? ***Yes*** or No
- Apply to ALL message types? ***Yes*** or No

Services that DO NOT apply to ANY Message

- The following services may apply at the enterprise, system, software, environmental, personnel, etc. but do not apply to the security requirements around any message type.
- Consensus work for applying security services started and completed on 02/02/2012.

Certification - Enterprise Credentials

- The assessments conducted in support of accreditations for enterprise credentials, conducting an impartial assessment of an enterprise credential.

- **NOT applied to ANY messages**

Certification - Enterprise Public Key

- The assessments conducted in support of accreditations for enterprise public key credentials, conducting an impartial assessment of an enterprise public key credential.

- **NOT applied to ANY messages**

Certification and Accreditation

- Evaluating, describing, testing and authorizing smart grid systems and services prior to or after a system is in operation.

- **NOT applied to ANY messages**

Environmental Security

- Ensuring environmental services are operational.

- **NOT applied to ANY messages**

Personnel Security

- Ensuring qualified personnel are retained to perform assigned responsibilities.

- **NOT applied to ANY messages**

Replication and Backup - Software

- Ensuring smart grid software is recoverable following an event.

- **NOT applied to ANY messages**